# National Infrastructure Protection Center CyberNotes

*Issue #24-99* *November 24, 1999*

**CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices.**

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

## *Bugs, Holes & Patches*

The following table provides a summary of software vulnerabilities identified between November 4, and November 18, 1999. The table provides the hardware/operating system, equipment/software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates from previous issues of CyberNotes are listed in bold. New information contained in the update will appear as red and/or italic text.**

| Hardware/ Operating System/ Vendor | Equipment/ Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| 3Com[1] | Palm HotSync Manager 3.0.4 under Windows 98 | The Palm Hotsync Manager is vulnerable to a buffer overflow attack that can crash the Hotsync application and possibly be used to execute arbitrary code on the machine running the Hotsync. | Solution: Block those ports from outside communication | HotSync Vulnerability | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |

[1] Securiteam, November 4, 1999.

| Hardware/ Operating System/ Vendor | Equipment/ Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| Admiral Systems, Inc.[2] | EmailClub 1.05 | Certain versions of EmailClub are vulnerable to a remote buffer overflow. This buffer overflow is exploitable via EmailClub's POP3 server, which fails to perform proper bounds checking on the 'From:' header on incoming e-mail. | No workaround or patch available at time of publishing. | E-MailClub Buffer Overflow Vulnerability | Low | Bug discussed in newsgroups and websites. Exploit has been published. |
| Antelope Software[3] | W4-Server 2.6a/Win32 | Certain versions of the W4-Server 32-bits personal webserver were shipped with a flawed script, Cgitest.exe, which fails to perform bounds checking on user supplied data and is vulnerable to a buffer overflow. | No workaround or patch available at time of publishing. | Cgitest.exe Buffer Overflow Vulnerability | Low | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Apple[4] | MacOS 9.0 | The NDS client for MacOS 9 fails to log the user out of the NDS tree when he/she logs out of the MacOS 9 system. The next user to log in to the machine will inherit the previous user's NDS access. | No workaround or patch available at time of publishing. Unofficial workaround: Always log out of NDS first. | NDS Client Inherited Login Vulnerability | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| Apple[5] | Microsoft Outlook Express for MacOS 5.0 | A security gap in Open Express 5.0 makes it possible for a malicious user to send (a multilingual HTML) message to an OE 5 user that will automatically download a file to the user's default Download folder without the OE 5 user's knowledge. | No workaround or patch available at time of publishing. | Outlook Express Mac Download Vulnerability | **High** | Bug discussed in newsgroups and websites. Vulnerability has appeared in the Press. |
| Artisoft[6] | XtraMail 1.11 | There are several potential buffer overflows that will crash the server and cause a Denial of Service. | No workaround or patch available at time of publishing. | Denial of Service Vulnerability | Low | Bug discussed in newsgroups and websites. Exploit has been published |

[2] SecurityFocus, November 16, 1999.
[3] SecurityFocus, November 16, 1999.
[4] SecurityFocus, November 14, 1999.
[5] SecurityFocus, November 16, 1999.
[6] USSR Labs, November 10, 1999.

| Hardware/ Operating System/ Vendor | Equipment/ Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| Cobalt[7] | RaQ2 | A vulnerability in the cgiwrap application shipped with Cobalt RaQ2 systems may let local sites steal data and requests from other locally hosted sites. The problem stems from the fact that cgiwrap will prefer to reference user applications before other web site applications. | Cobalt has an updated package available on their ftp site located at: ftp://ftp.cobaltnet.com/pub/experimental/secuirty/ | CGIwrap Vulnerability | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| DataFellows[8] | SSH Communi-cations Security SSH 1.2.27 | It is possible to overflow one of the internal buffers of SSH 1.2.27, causing the program to crash and possible execute arbitrary code. This version is no longer supported. | The latest version of SSH (Server) can be downloaded from: http://www.datafellows.com/products/cryptography/f-sshserver.htm | Remote Buffer Overflow Vulnerability | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Debian[9] | GNU/Linux 2.1 | Proftpd has several buffer overflow vulnerabilities that could be exploited by remote attackers. | Upgrade your Proftpd package with version 1.2.0pre904 which can be found at: http://security.debian.org/dists/stable/updates/binary-/proftpd_1.2.0pre9-4 Please select the appropriate architecture for your system. | Proftpd Remote Exploit Vulnerabilities | Low | Bug discussed in newsgroups and websites. |
| DeleGate[10] | DeleGate 5.9.7 and prior; 6.0.1 | A buffer overflow exists that may allow a remote malicious users to execute arbitrary code. | No workaround or patch available at time of publishing. | Remote Buffer Overflow Vulnerability | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Eric Allman[11] | Sendmail 8.8.x | Through exploiting a combination of vulnerabilities in Sendmail, it is possible for a malicious local user to have an arbitrary program inherit (or 'hijack') the file descriptor for the socket listening on (privileged) port 25. | Upgrade to the latest version 8.9.3. | Sendmail Socket Hijack Vulnerability | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |

[7] Bugtraq, November 8, 1999.
[8] Securiteam, November 17, 1999.
[9] Bugtraq, November 11, 1999.
[10] Securiteam, November 17, 1999.
[11] SecurityFocus, November 5, 1999.

| Hardware/ Operating System/ Vendor | Equipment/ Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| **Etype**[12]<br><br>***A new version of Eserv is now available.***[13] | **Eserv 2.50** | **An unauthorized user can gain read access to any file on the system, including account files, by entering a specific string in a URL.** | **No workaround or patch available at time of publishing.**<br><br>***A new version of Eserv is available at:*** ftp://ftp.eserv.ru/eserv/pub/Eserv2841.zip<br>***Also for users who do not wish to upgrade there is a patch. Patch information is available at:*** ftp://ftp.eserv.ru/eserv/pub/autorun-www.txt | **Eserv 2.5 Directory Traversal Vulnerability** | **Medium / High** | **Bug discussed in newsgroups and websites. Exploit has been published. Trojan Horse program exists that looks for the specific port.**<br><br>***Exploit script has been published.*** |
| F5 Networks[14] | BIG/ip 2.1, 2.1.2 | BIG/ip contains a default password that a unauthorized user could guess resulting in a system compromise.<br><br>It is also possible to view any file to which BIG/ip's administration HTML interface has access to | Instructions for fixing this vulnerability along with the patch can be found at: www.Tech.f5.com/home/passwordchange.html | BIG/ip Security Vulnerabilities | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| **Floosietek**[15]<br><br>***New version/fix available.***[16] | **FTGate 2.1** | **An unauthorized user can gain read access to any file on the system, including account files, by entering a specific string in a URL.** | **No workaround or patch available at time of publishing.**<br><br>***Upgrade to the latest release, or only bind the web interface to 'trusted' interface.***<br>***FTGate version 2.2 is available, at:*** Http://www.floosietek.com/dl_ftg/download.htm | **FTGate 2.1 Directory Traversal Vulnerability** | **Medium / High** | **Bug discussed in newsgroups and websites. Exploit has been published. Trojan Horse program exists that looks for the specific port.** |
| FreeBSD[17] | FreeBSD 3.3 | A vulnerability exists in seyon v2.14b, which will allow any user to upgrade his/hers, privileges to the privileges seyon runs with. | No workaround or patch available at time of publishing.<br>Unofficial workaround:<br>Do:<br>$ chmod 750 'which seyon'<br>And add only selected users to the "dialer" group. | Seyon Privilege Elevation Vulnerability | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |

[12] NTBUGTRAQ, November 4, 1999.
[13] SecurityFocus, November 16, 1999.
[14] Securiteam, November 10, 1999.
[15] USSR Labs, November 5, 1999.
[16] Bugtraq, November 10, 1999.
[17] Bugtraq, November 8, 1999.

| Hardware/ Operating System/ Vendor | Equipment/ Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| Gene6[18] | G6 FTP Server 2.0 (Beta 4/5) | The G6 FTP Server is vulnerable to a buffer overflow attack. If 2000 characters are sent as the username or password, the software will use up all available memory and CPU time and bring the host to a halt. | No workaround or patch available at time of publishing. | G6 FTP Server Buffer Overflow Vulnerability | Low | Bug discussed in newsgroups and websites. Exploit has been published. |
| ImmuniX[19] | StackGuard | A security vulnerability exists that could permit a malicious user to successfully compromise StackGuarded programs. | Upgrade to StackGuard 1.21 which is available at: http://imunix.org/downloads.html#sql.21 | StackGuard Evasion Vulnerability | Medium/ Low | Bug discussed in newsgroups and websites. Exploit has been published. |
| International TeleCommuni-cations[20] | WebBBS 2.13 | In certain versions of WebBBS a buffer overflow condition exists in the initial login program. User supplied data via the login name and password are not bounds checked which could lead to a compromise of the system running WebBBS. | No workaround or patch available at time of publishing. | WebBBS Login & Password Buffer Overflow Vulnerability | Low | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Interscan[21] | VirusWall 3.23, 3.3 | A buffer overflow vulnerability exists in Interscan's VirusWall SMTP gateway, which could possibly allow execution of arbitrary code. | Patch available at: http://download.antivirus.com/ftp/products/patches/isvw331_patch.zip | Interscan Virus Wall Buffer Overflow Vulnerability | **High** | Bug discussed in newsgroups and websites. Exploit scripts have been published. |
| IPSwitch[22] | Imail 5.0.5, 5.0.6, 5.0.7 | Due to improper bounds checking, a buffer overflow occurs when a lengthy username is sent. | Patch can be found at: ftp://ftp.ipswitch.com/lpswitch/Product_Support/Imail/imail508.exe | POP3 Buffer Overflow Vulnerability | Low | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Irfan[23] | Image Viewer 3.07 | A buffer overflow condition exists when Image viewer handles Adobe PhotoShop image files. This makes it possible possibly to execute arbitrary code. | Patch can be found at: http://stud1.tuwien.ac.at/~e9227474/iview310.zip | Buffer Overflow Vulnerability | **Medium** | Bug discussed in newsgroups and websites. Exploit has been published. |

[18] USSR Labs, November 17, 1999.
[19] Bugtraq, November 9, 1999.
[20] SecurityFocus, November 16, 1999.
[21] Securiteam, November 9, 1999.
[22] SecurityFocus, November 10, 1999.
[23] Securiteam, November 15, 1999.

| Hardware/ Operating System/ Vendor | Equipment/ Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| Linux[24] | Alpha Linux | Alpha Linux contains a buffer overflow vulnerability. | No workaround or patch available at time of publishing. | Alpha Linux buffer Overflow Vulnerability | Low | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Linux[25] | RedHat Linux 4.x, 5.x; Debian GNU/Linux 2.1; universal NFS Server 2.2beta46 and below | It is possible to overflow NFSd's path+filename string buffer, causing the program to crash and execute arbitrary code, by creating a very large directory structure and a very long file name. | Contact your vendor for security fix/patch. | Buffer Overflow Vulnerability | Medium/ **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Microsoft[26] | Internet Explorer 5.0 for Windows 95/98/NT 4.0 | The Windows Media Player ActiveX control returns a specific error code if it is instructed to load a local file that does not exist. A malicious user could utilizes this behavior to gather information about the system. | No workaround or patch available at time of publishing. Unofficial workaround is to disable active scripting. | ActiveX Error Message Vulnerability | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| Microsoft Windows[27] | Windows 95/98 | A vulnerability in Windows 95/98 exists which allows a web site or E-mail message to cause the Windows machine to crash, or possibly run arbitrary code. | Patch available at: Windows 95 http://download.microsoft.com/download/win95/update/245729/w95/en-us/245729us5.exe Windows 98 http://download.microsoft.com/download/win98/update/245729/w98/en-us/245729us8.exe | File Access URL Vulnerability | **High** | Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the Press. |
| **Microsoft Windows 95, 98, 2000, and NT 4.0[28]** ***Microsoft re-releases JavaScript Redirect Vulnerability.*** [29] | **Microsoft Internet Explorer 4.0.1, 5.0** | **A vulnerability exists in Internet Explorer that could allow a malicious web site operator to read files on the computer of a user who visited the site** | **Microsoft has released a patch for this vulnerability which is available at: http://www.microsoft.com/security/bulletins/MS99-046faq.asp.** ***Patch Availability:*** http://www.microsoft.com/downloads | **JavaScript Redirect Vulnerability** | **Medium** | **Bug discussed in newsgroups and websites. Exploit script has been published.** |

[24] Bugtraq, November 13, 1999.
[25] RedHat Security Advisory, RHSA-1999:053-01, November 11, 1999.
[26] SecurityFocus, November 14, 1999.
[27] Microsoft Security Bulletin, MS99-049, November 12, 1999.
[28] Microsoft Security Bulletin, MS99-043, October 18, 1999.
[29] Microsoft Security Bulletin, MS99-043, November 17, 1999.

| Hardware/ Operating System/ Vendor | Equipment/ Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| Microsoft Windows 95/98/NT 4.0[30] | Microsoft Outlook 98, 2000; Microsoft Outlook Express 4.27.3110.1, 4.72.2106.4, 2.72.3120.0, 4.72.3612.1700 | Vulnerability exists in Outlook and Outlook Express, which allows remote malicious users to execute arbitrary code on the user's machine if JavaScript is enabled. A malicious user can create an executable file, compress it into a CAB file, and rename it to have a multimedia file extension. He can then send this file as an attachment to an Outlook user as well as some JavaScript code. When the user double-clicks on the multimedia attachment it will save the executable file in a known location on the system. The JavaScript will then execute the attachment on the target machine. | To fully quash this vulnerability, Microsoft recommends the active setup control patch located at: http://www.microsoft.com/msdownload/iebuild/ascontrol/en/ascontrol.htm Please see Microsoft Security Bulletin (MS99-048) Frequently Asked Questions located at: http://www.microsoft.com/security/bulletins/MS99-048faq.asp | ActiveX CAB File Execution Vulnerability | **High** | Bug discussed in newsgroups and websites. Exploit script has been issued. **This is the 'BubbleBoy' exploit .** Vulnerability has appeared in the Press. |
| Microsoft Windows 98/NT[31] | WordPad | Win98/NT4 Riched20.dll (which WordPad uses) has a buffer overflow problem with ".rtf"-files, which could result in executing arbitrary code. The code can be put into a .rtf file and mailed to the victim. | No workaround or patch available at time of publishing. | WordPad Buffer Overflow Vulnerability | Medium/ **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Microsoft Windows NT[32] | NT Service Pack 6 | A vulnerability exists in SP6 which prevents users from accessing Lotus Notes and Wall Data's "Rumba" without administrator rights (the highest and broadest level of network access), unless companies compromise security. | Customers using these applications should install the corresponding Alpha or X86 hotfix after installing SP6. For more information on this issue, please read Microsoft KB Article Q245678 located at: http://support.microsoft.com/support/kb/articles/Q245/6/78.asp | Windows NT Update Vulnerability | **High** | Bug discussed in newsgroups and websites. Vulnerability has appeared in the Press. |
| Microsoft Windows NT[33] | SQL Server 7.0 | The SQL Server 7 encrypt() function is trivial to break with a plaintext attack. | No workaround or patch available at time of publishing. | Linked Server Password Vulnerability | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |

[30] SecurityFocus, November 8, 1999.
[31] Bugtraq, November 18, 1999.
[32] Bugtraq, November 16, 1999.
[33] Bugtraq, November 15, 1999.

| Hardware/ Operating System/ Vendor | Equipment/ Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| **Microsoft Windows NT 4.0**[34]<br><br>***Microsoft issues a fix.***[35]<br><br>***Patch removed from download site.***[36] | **Microsoft TCP/IP Stack for NT 4.0 up to and including SP3** | **Windows NT 4 uses predictable TCP sequence number generating algorithms that could allow an attacker to set up connections to other machines with a spoofed source address of the NT host.**<br><br>***Microsoft had determined that the patch contains a regression error and has removed it from the download site.*** | **No workaround or patch available at time of publishing.**<br><br>***Patch available at:*** **http://www.microsoft.com/security/bulletins/ms99-046.asp**<br><br>***A new version of the patch is expected to be released soon.*** | **TCP/IP Sequence Numbering Vulnerability** | **Medium** | **Bug discussed in newsgroups and websites. Exploit has been published.** |
| NetcPlus Internet Solutions, Inc.[37] | SmartServer3 3.5.1 | The POP server that is part of the NetcPlus SmartServer 3 e-mail server has an unchecked buffer that could allow an attacker to execute arbitrary code on the server. | NetcPlus is soon releasing SmartServer3 version 3.60, which fixes this vulnerability. | SmartServer3 POP Buffer Overflow Vulnerability | **High** | Bug discussed in newsgroups and websites. Exploit scripts have been published. |
| Network Solutions[38] | NetSol | A vulnerability exists with handling of passwords for CRYPT-PW authentication. | No workaround or patch available at time of publishing. | Insecure Password Handling Vulnerability | Medium | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Oracle[39] | Oracle7 7.3.3, 7.3.4; Oracle8 8.05, 8.1.5; Oracle Application Server 4.0.x | Multiple root compromise vulnerabilities exist in Oracle Application Server. | Oracle customers can find important information on Oracle's web-based Metalink system at: http://metalink,oracle.com. Customers should reference document number 76484.1 under the advanced search engine available on Metalink. | Multiple Root Compromise Vulnerabilities | **High** | Bug discussed in newsgroups and websites. Exploit scripts have been issued. |
| QPC Software[40] | QVT/Term Plus 4.2d FTP Server | The FTP server is vulnerable to a Denial of Service attack. | No workaround or patch available at time of publishing. | Denial of Service Vulnerability | Low | Bug discussed in newsgroups and websites. Exploit has been published. |

[34] Securiteam, August 28, 1999.
[35] Microsoft Security Bulletin, MS99-046, October 22, 1999.
[36] Microsoft Produce Security, November 17, 1999.
[37] BindView Security Advisory, November 11, 1999.
[38] Bugtraq, November 8, 1999.
[39] ISS Security Advisory, November 10, 1999.
[40] USSR Labs, November 10, 1999.

| Hardware/ Operating System/ Vendor | Equipment/ Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| RedHat[41] | Linux 6.1 | A vulnerability exists in login if you are using csh/tcsh, which makes it possible to execute arbitrary commands. The problem has to do with the Initscripts for these shells that run when the user logs in and a /tmp race condition which they are vulnerable to. | Upgrade your Initscripts package: ftp://updates.redhat.com/6.1/i386/initscripts-4.63-1.8386.rpm | Tmp Race Vulnerability | **High** | Bug discussed in newsgroups and websites. |
| Tektronix[42] | PhaserLink 740.0 | A vulnerability exists which shows the administrator password to anyone without authentication. This password can be bypass to directly reconfigure the printer. | No workaround or patch available alt time of publishing. Unofficial workaround: Block Port 80 access to this printer via a router or firewall, or disable the PhaserLink webserver on the printer. | PhaserLink Webserver Vulnerability | Low | Bug discussed in newsgroups and websites. Exploit has been published. |
| TransSoft[43] | Broker FTP Server 3.5 | A remote malicious user can initiate a Denial of Service attack. This attack is in the form of a buffer overflow caused by a long user name of 2730 characters. | No workaround or patch available at time of publishing. | Denial of Service Vulnerability | Low | Bug discussed in newsgroups and websites. Exploit has been published. |
| University of Kansas[44] | Lynx 2.7, 2.8 | Lynx contains a security vulnerability that allows malicious users to change the configuration settings of Lynx and potentially gaining of access to other people's accounts. | No workaround or patch available at time of publishing. | Parameter/ internal Link Verification Vulnerability | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| Unix[45] | BIND 8.2.2 and prior | Six vulnerabilities exist in BIND, which make it vulnerable to root compromises, DoS attacks, cache poisoning and more. | Apply a patch from your vendor or update to a later version of BIND. | Multiple BIND Vulnerabilities | **High** | Bug discussed in newsgroups and websites. Exploit script has been released. |
| Unix[46] | THTTPSd 2.04 and prior | Trivial HTTP (THTTPd) contains an remote buffer overflow, which allows remote malicious users to crash the HTTP server and possibly execute arbitrary code. | 2.05 can be downloaded from: http://www.acme.com/software/thttpd/thttpd-2.05.tar.gz SuSE has released a fixed package at: Suse 6.2: ftp://ftp.suse.com/pub/suse/j8386/update/6.2/nl/thttpd-2.04-31.i386.rpm SuSE 6.3 ftp://ftp.suse.com/pub/suse/j8386/update/6.3/nl/thttpd-2.04-31.i386.rpm | Remote Stack Overflow Vulnerability | **High** | Bug discussed in newsgroups and websites. |

[41] Red Hat, Inc. Security Advisory, RHSA-1999:052-01, November 8, 1999.
[42] Bugtraq, November 16, 1999.
[43] USSR Labs, November 8, 1999.
[44] SecurityFocus, November 17, 1999.
[45] CERT Advisory CA-99-14, November 12, 1999.
[46] SecurityFocus, November 9, 1999.

| Hardware/ Operating System/ Vendor | Equipment/ Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| Unix[47] | WU-FPT 2.4.x | When using the cd (CWD) command to a user's home directory, the WU-FTPD will reveal the physical path of the home directory and whether the account is a standard account such as root, games, uucp, etc. For non-standard or non-existent accounts, the FTP daemon will claim not to know the user. | No workaround or patch available at time of publishing. | User Information Vulnerability | Low | Bug discussed in newsgroups and websites. Exploit has been published. |

*Risk is defined in the following manner:

**High -** A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

**Medium -** A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

**Low -** A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

## *Recent Exploit Scripts/Techniques*

The table below contains a representative sample of exploit scripts and How to Guides, identified between November 4, and November 18, 1999, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that hackers/crackers are utilizing**. During this period, 118 scripts, programs, and net-news messages containing holes or exploits were identified.

| Date of Script (Reverse Chronological Order) | Script Name | Script Description | Comments |
|---|---|---|---|
| **November 18, 1999** | **Cgi-check99v4.r** | **Scanner which checks for 119 remote CGI vulnerabilities and other remote issues.** | |
| **November 18, 1999** | **Lynx-2.8.x.txt** | **Exploit technique that can be used against the Lynx vulnerability, which can result in a local compromise.** | |

[47] Securiteam, November 7,1999.

| Date of Script (Reverse Chronological Order) | Script Name | Script Description | Comments |
|---|---|---|---|
| **November 18, 1999** | **Wordpad.txt** | **Exploit technique that can be used against the Microsoft WordPad Buffer Overflow vulnerability.** | |
| November 17, 1999 | Brscan06.c | Scans internal network for systems running certain services without running a full-blown portscan. This allows you to scan an IP address range for a specific port. | |
| **November 17, 1999** | **G6ftp.dox.txt** | **Remote exploit technique that can be used against the G6 FTP Server Buffer Overflow Vulnerability.** | |
| November 17, 1999 | Icq.txt | Tutorial for ICQ cracks and how they actually work. | |
| November 16, 1999 | Autoexec.bat | Etype Eserve directory transversal vulnerability script. | |
| **November 16, 1999** | **Ex_emc.c** | **Exploit script for the E-MailClub Buffer Overflow Vulnerability.** | |
| **November 16, 1999** | **Ex_w4server.c** | **Exploit script for the W4 Server Cgitest.exe Buffer Overflow Vulnerability.** | |
| **November 16, 1999** | **Ex_webbbs.c** | **Exploit script for the WebBBS login and password Buffer Overflow Vulnerability.** | |
| **November 16, 1999** | **Nessux-0.99.1.tar.gz** | **Multithreaded remote security scanner for Linux, BSD, Solaris.** | |
| **November 15, 1999** | **Alpha-bof.txt** | **A technique paper, which explains how to exploit a buffer, overflow under Alpha Linux.** | |
| November 15, 1999 | Bdoor.c | Unix backdoor which pretends to be a http daemon. | |
| November 15, 1999 | Bug02.tgz | A spy program for Linux, which reads from the microphone and sends the audio back to the client in UDP packets. | |
| **November 15, 1999** | **Delefate.c** | **Remote exploit script for DeleGate 5.9x – 6.0x vulnerability.** | |
| November 15, 1999 | GHost.v1-al-tgz | Thorough set of remote security scanning scripts. | |
| November 15, 1999 | IIS-ap.zip | Microsoft Access database password cracker. Works on Access 97 and 2000. | |
| November 15, 1999 | Knark-0.50.tar.gz | Kernel-based rootkit for Linux 2.2. Hides files in the filesystem, strings from/proc/net for netstat, processes, and program execution redirect. | |
| November 15, 1999 | Namedscan.0.0.tar.gz | Named version scanner. | |

| Date of Script (Reverse Chronological Order) | Script Name | Script Description | Comments |
|---|---|---|---|
| November 15, 1999 | Nbchk.pl | A multi-threaded perl banner-checking utility that is fully configurable and can scan a full/partial class-C network, hosts from a file, or a single host for configured vulnerabilities. | |
| November 15, 1999 | NSS_25.tar.gz | Narrow Security Scanner is a perl script, which checks for 177 remote vulnerabilities. | |
| November 15, 1999 | Oracle8.exploit.txt | Local root exploit shell script for Oracle 8 vulnerability. | |
| November 15, 1999 | Oracle-ex.c | Exploit script for Oracle version 8.0.5. | |
| November 15, 1999 | Oracle-linux.sh | Linux root compromise exploit script for Oracle. | |
| November 15, 1999 | Oracle-sol.sh | Oracle root compromise exploit script. | |
| **November 15, 1999** | **Qvtftp42-zip** | **Exploit script for the QVT/Term Plus 4.2d server Denial of Service vulnerability.** | |
| **November 15, 1999** | **Ss351exp.tgz** | **Windows binary and source exploit code for NetCPlus SmartServer3 POP 3.51.1 vulnerability.** | |
| **November 15, 1999** | **Ssh-1.2.27.txt** | **Technique that remotely exploits the buffer overflow vulnerability in ssh-1.2.27.** | |
| November 15, 1999 | Sslcrack.zip | A basic VB5 Win9x brute force PIN SSL cracker. Includes HomeBanking.txt, which explains a common weakness in Home Banking systems that allows brute forcing the PIN. | |
| November 13, 1999 | Oracle.sh | Exploit script for Oracle 8.1.5 on Solaris 2.6 and probable others. | |
| November 12, 1999 | Adm-nxt.c | ADM named 8.2/8/2.1 NXT remote overflow exploit. | |
| November 12, 1999 | Bind.nxt.txt | Exploit technique for the processing of NXT records in all versions of BIND below 8.2.2 which allows attackers remote access to DNS servers at the privilege level that the DNS server runs at. | |
| November 12, 1999 | Formhandler.cgi.txt | FormHandler-cgi uses hard coded physical path names for templates so it is possible to read any file on the system.. | |
| November 11, 1999 | Mcrash.tgz | Denial of Service exploit for the Windows Mailgate 3.2.114 vulnerability. | |
| November 10, 1999 | 3nfsd2.c | Rpc.nfsd2 exploit script for Linux. | |

| Date of Script (Reverse Chronological Order) | Script Name | Script Description | Comments |
|---|---|---|---|
| **November 10, 1999** | **Nic_crack.c** | **Script which brute forced NetSol encrypted NIC update passwords.** | |
| **November 10, 1999** | **Qvt-term.4.2.dox.txt** | **Remote Denial of Service attack in QVT/Term Plus 4.2d Vulnerability.** | |
| **November 10, 1999** | **Xtramail.dox.txt** | **Multiple remote Denial of Service attacks in Artisoft XtraMail v1.11 Vulnerability.** | |
| **November 9, 1999** | **Freebsd.seyon.txt** | **Exploit script for the seyon vulnerability.** | |
| **November 8, 1999** | **Brokerftp.txt** | **Technique for the Remote DoS Attack in TransSoft's Broker Ftp Server v3.5 Vulnerability.** | |
| November 8, 1999 | Cobalt.cgiwrap.txt | Technique for the "cgiwrap" program vulnerability on Cobalt RaQ2 Servers. | |
| November 8, 1999 | Godmessage.zip | Exploit of the Microsoft script lib bug and reg wiz control buffer overflow, which allows arbitrary code to be executed when this HTML is viewed. | |
| November 8, 1999 | Ie5.file.txt | Exploit for Japanese Windows 98 Microsoft Internet explorer 4/5 overflow vulnerability. | |
| November 8, 1999 | Imailpopx.c | Script which exploits the Imail POP3 Buffer Overflow Vulnerability. | |
| November 8, 1999 | Interscan.txt | VirusWall SMTP Gateway buffer overflow vulnerability exploit code. | |
| November 8, 1999 | Irfan.view32.txt | Code which exploits the Irfan Imager Viewer. | |
| November 8, 1999 | Kmap-0.6.1.tar.gz | AA popular and powerful console portscanner. | |
| November 8, 1999 | Spynet206.exe | SpyNet is a sniffer for Windows 95/98, which can recompose the original TCP sessions from the composing packets. | |
| November 8, 1999 | Targa3.c | A Denial of Service exploit that sends random IP packets with parameters known to cause crashes on various machines and can be used to determine if a systems IP stack is really stable and crash-proof under unexpected conditions. | |
| November 8, 1999 | Vwxploit.c | Unix port of Interscan Virus wall 3.23/3.3 remote exploit. | |
| November 8, 1999 | Vwxploit.zip | NT binary and asm source code to Interscan VirusWall 3.23./3.3 remote exploit. | |
| November 5, 1999 | Amloger.c | An auto logger for Amuser-net BBS which is used in the many Japanese underground sites. | |

| Date of Script (Reverse Chronological Order) | Script Name | Script Description | Comments |
|---|---|---|---|
| November 5, 1999 | Cgiexp.c | This utility lists the servers, which have the security vulnerabilities of CGI programs. This utility supports the pht, test-cgi, nph-test-cgi, campas, htmlscript, service, pwd. The addition of new vulnerabilities is very easy. | |
| November 5, 1999 | Easyscan.c | A simple full-connection TCP port scanner. This utility lists the servers that open the specified port. | |
| November 5, 1999 | Ex_almail.c | Overflow vulnerability exploit for AL-Mail32. | |
| November 5, 1999 | Ex_canuum.c | Local root exploit code for the buffer overflow vulnerability in canuum for Japanese Linux. | |
| November 5, 1999 | Ex_chocoa.c | Script which exploits the overflow vulnerability in CHOCOA 1.0beta7R. | |
| November 5, 1999 | Ex_dtprintinfo86.c | Script which exploits a stack buffer overflow present in x86 version of Solaris 2.6 and 2.7. Local root compromise | |
| November 5, 1999 | Ex_fuse.c | Exploit code that executes any command on the host, which is running the Cmail FuseMail 2.7. | |
| November 5, 1999 | Ex_hpprint.c | Exploit script for the overflow vulnerability in IBM HomePagePrint 1.0.7. | |
| November 5, 1999 | Ex_ie4.c | Exploit script for the Microsoft Internet explorer 4/5 overflow vulnerability. | |
| November 5, 1999 | Ex_lpset86.c | Local root exploit code for the buffer overflow vulnerability in lpset for Solaris x86 machines. | |
| **November 5, 1999** | **Ex_netsrv.c** | **Exploit code that executes any command on the host, which is running the NetcPlus SmartServer3.** | |
| November 5, 1999 | Ex_nextftp.c | Exploit script for the overflow vulnerability in NextFTP Version 1.82. | |
| November 5, 1999 | Ex_pms.c | Personal Mail Server overflow vulnerability exploit script. | |
| November 5, 1999 | Ex_pms-tr.c | Another personal mail server remote exploit. | |
| November 5, 1999 | Ex_sdtcm_convert.c | Local root exploit for buffer overflow condition in sdtcm_convert for Solaris Sparc machines. | |
| November 5, 1999 | Ex_sdtcm_convert86.c | Local root exploit for the buffer overflow condition in sdtcm_convert for Solaris x86 machines. | |
| November 5, 1999 | Ex_servu.c | Windows 98 buffer overflow exploit script for the Serv-U Version 2.5 ftp daemon vulnerability. | |

| Date of Script (Reverse Chronological Order) | Script Name | Script Description | Comments |
|---|---|---|---|
| November 5, 1999 | Ex_tinyftpd.c | Exploit code that executes any command on the host, which is running the TinyFTPd Ver0.51. | |
| November 5, 1999 | Ex_uum.c | Local root exploit code for the buffer overflow in uum for Japanese Linux. | |
| November 5, 1999 | Ex_zommail.c | Exploit script for the overflow vulnerability in Zom-Mail 1.09. | |
| November 5, 1999 | Ex-admintoolc. | Admintool local root exploit for Solaris 2.6/7 Sparc machines. | |
| November 5, 1999 | Ex-ie5.c | Overflow exploit for IE5. | |
| **November 5, 1999** | **Ex-imagemap.c** | **Buffer overflow exploit script for OmniHTTPd.** | |
| November 5, 1999 | Extusr.zip | This utility extracts the username and makes a userlist file from the html file of "user's page" which can be often seen at the ISP's web page. | |
| November 5, 1999 | Ftpt.c | Ftp Trojan logs the hostname, username, and password when the local users use the ftp. | |
| November 5, 1999 | Gscan.c | A generic banner scanner. | |
| November 5, 1999 | Hrs100.c | This program will be rootshell if you specify the special argment. If the special argment is not specified, this program calls a specified program. | |
| November 5, 1999 | http_logadd.c | This program can add the fake log to HTTPd remotely. | |
| November 5, 1999 | Iesrc.zip | Source Viewer Changer for Internet Explorer 5. | |
| November 5, 1999 | Irixaa.tar.gz | This program checks many IRIX security holes automatically. This scanner contains the ttdbserver attack. | |
| November 5, 1999 | Itelnet.tar.gz | Telnet Trojan based on GNU telnet. This Trojan can be installed with non-root user, if the user account is used by many crackers, you can also know the cracking process and the location of rootshell. | |
| November 5, 1999 | Jsy.zip | Brute force attacker ShirakiYoko for Java. | |
| November 5, 1999 | Kakarityo.lzh | ICQ tool for Win32 that can retrieve IP address and port by UIN. | |
| November 5, 1999 | Logchk.c | Utility which shows you all entries, you can analyze the logfile. | |

| Date of Script (Reverse Chronological Order) | Script Name | Script Description | Comments |
|---|---|---|---|
| November 5, 1999 | Minatomirai101.lzh | This is a GUI-based full connect port scanner for Windows 95/98/NT. | |
| November 5, 1999 | Oshare1.c | Exploit code to crash (BSOD) Windows 98 machines with malformed packets. | |
| November 5, 1999 | Passwd_freebsd.c | Passwd Trojan for FreeBSD. | |
| November 5, 1999 | Passwd_irix.c | Paswd Trojan for IRIX. | |
| November 5, 1999 | Passwd_linux.c | Passwd Trojan for Linux. | |
| November 5, 1999 | Passwd_solaris.c | Passwd Trojan for Solaris2.x | |
| November 5, 1999 | Passwd_sunos4.c | Passwd Trojan for SunOS4. | |
| November 5, 1999 | Rbackdoor.c | A backdoor program that can be accessed remotely as telnetd. | |
| November 5, 1999 | Rch.zip | Small and useful Trojan or Win32. | |
| November 5, 1999 | Sendexp.c | Exploit code that can send and execute a Trojan program, which is prepared in the attacker host. The programs sends the ".exe" program to the victim host, and the exploit code executes it. | |
| November 5, 1999 | ShadowScan.zip | This is a program intended for the analysis IP of networks, including also services, attacks, the passwords guessing for POP3 & FTP. | |
| November 5, 1999 | Simplestealth.c | This is the simple half-open and stealth TCP port scanner. | |
| November 5, 1999 | Sut.c | SU Trojan version 2.00. | |
| November 5, 1999 | Sut_digital.c | SU Trojan for Digital. | |
| November 5, 1999 | Sut_irix.c | SU Trojan for IRIX. This Trojan logs the passwords. If you install the su Trojan correctly, local users or admin fails the first "su", and the password which is imputed to SU Trojan has been logged to the specified file. | |
| November 5, 1999 | Sut_sol24.c | SU Trojan for Solaris 2.4. | |
| November 5, 1999 | Sut_sol25j.c | SU Trojan for Solaris 2.5. | |

| Date of Script (Reverse Chronological Order) | Script Name | Script Description | Comments |
|---|---|---|---|
| November 5, 1999 | Sut_sun41.c | SU Trojan for SunOS4. | |
| November 5, 1999 | Tcpshell.c | A backdoor program which can be accessed remotely as telnetd. | |
| November 5, 1999 | Tdm.c | A backdoor program which can be accessed remotely as telnetd. You can login without username and password to the host which program is installed. This program can also use as CGI program if you send the compiled binary and change the permission to 755. | |
| November 5, 1999 | Udp_shell.tar.gz | UDP based backdoor which supports the Unix shell command. | |
| November 5, 1999 | Udpscan.c | Simple UDP port scanner based on the ICMP. | |
| November 5, 1999 | Ulw.c | Log wiper, which wipes the log entry of wtmp, wtmpx, utmp, utmpx, lastlog without such wiped traces. This utility can also reconstruct the zapped logs and remove the null entry. | |
| November 5, 1999 | Upgrade.sendmail.8x.txt | Denial of Service exploit technique for the Sendmail vulnerabilities. | |
| November 5, 1999 | Uzapper.c | This is the general log wiper for Solaris, SunOS, IRIX, Linux, and FreeBSD. | |
| November 5, 1999 | Xifconfig.c | This program fakes the ifconfig command, the PROMISC message will not be shown. | |
| November 5, 1999 | Xtcp200.lzh | A remote backdoor for Windows 95/98/NT as a Unix shell services. You can get/put/remove/copy/execute the files, and shutdown, reboot the PC. | |
| November 5, 1999 | Yoko125.tar.gz | Utility, which searches joe-accounts for, specified host using ftp bluteforce attack based on userlist file. This utility also can attack by using the fixed password and username+string. | |
| November 5, 1999 | Yoko130.zip | This utility searches joe-accounts for specified host using ftp and pope bruteforce attack based on the userlist file. This utility also can attack by using the fixed password, username+string, and reversed username. | |
| **November 4, 1999** | **Hotsync.manager.txt** | **The Palm Hotsync manager buffer overflow vulnerability.** | |
| November 4, 1999 | Ie.50.redirection.txt | Exploit details for the Internet Explorer 5.0 vulnerability. | |
| November 4, 1999 | Ie.40.redirection.txt | Exploit technique that can be used against the Internet explorer 4.0 vulnerability which allows reading local text and HTML files. | |

| Date of Script (Reverse Chronological Order) | Script Name | Script Description | Comments |
|---|---|---|---|
| November 4, 1999 | Rfpoison.py | Services.exe Denial of Service ported to python. | |
| November 4, 1999 | Spoolsploit.zip | Windows NT spoolss.exe exploit. | |

## Script Analysis

This section will supply a short description of scripts that have been analyzed by various security professionals and organizations. If you or your organization wish to contribute, please send e-mail to nipc@fbi.gov with the subject line "CyberNotes Script Analysis." While this section will list only short descriptions, contributors are requested to include a full technical analysis of the script along with release instructions. The release categories are: releasable to anyone; limited releasability (originator-defined list of organizations); or provided for NIPC only. If you would like to receive a copy of the full technical analysis version of any summarized analysis, please send an e-mail listing the script name and requesting the full technical analysis. A member of the CyberNotes editorial team will contact you. All contributions will be credited to the contributing individual or organization unless otherwise requested.

## Trends

**Trends for this two week period:**

- **Numerous sites are being compromised via vulnerabilities in IIS web servers and MS Data Access Components (MDAC) vulnerabilities. (CyberNotes 99-22).** The Microsoft Data Access Components (MDAC), a part of Windows NT, and the RDS (Remote Data Services) DataFactory object vulnerabilities are currently the primary means for successful attacks on NT systems.
- An increase in widespread probes to port 98/tcp has been seen.
- We have received reports about intruders compromising machines in order to install distributed systems used for launching packet-flooding Denial of Service attacks. Two of the tools being used are trinoo and tribe flood network (or TFN). These tools appear to be undergoing active development, testing and deployment on the Internet.
- Two vulnerabilities are being used together to gain access to vulnerable systems. The first is rpc.statd, a program used to communicate state changes among NFS clients and servers. The second is in automountd, a program used to automatically mount certain types of file systems.
- Intrusion detection systems ranging from home computers with cable modems to high-end government facilities have been reporting a large number of probes to TCP ports 80, 8080 and 3128.
- Variations of the Melissa virus continue to appear.
- Intruders are using distributed network sniffers to capture usernames and passwords. UDP packets containing username and password information may be sent to one or more remote sniffer servers using source port 21845/udp.
- Increased intruder activity has been noticed involving the am-utils package.
- An increase in widespread probes to port 21/tcp has been seen.

## Viruses

**BubbleBoy:** A new e-mail worm proves that you no longer have to open an attachment to infect your system with a virus. Once activated, BubbleBoy will send itself to every contact in the Outlook or Outlook

Express e-mail address book, but the current version of the worm does not carry a destructive payload. Thus, users may not immediately realize they have been infected. The only visible effects are that the system's registered owner and organization are changed, via the registry, to "BubbleBoy" and "Vandelay Industries", respectively.

The worm arrives as e-mail with the "from" line referring to the person who unintentionally sent it and the subject line: "BubbleBoy is back!"

The body of the e-mail, when opened, will contain a black screen and the text, "The BubbleBoy incident, pictures and sounds," along with an invalid URL ending in "bblboy.htm." To infect a system, the worm requires Internet Explorer 5 with Windows Scripting Host installed, which is standard in Windows 98 and Windows 2000 installations. It does not seem to run on Windows NT, at this time. If using Outlook, the worm requires that you "open" the email, and will not run if the email is viewed through the "Preview Pane." If Outlook Express is used, the worm activates even if the email is only viewed through the "Preview Pane." In all cases, if the security settings for the Internet Zone in IE5 are set to High, the worm will not be executed.

After infection, BubbleBoy will set a registry key to indicate that the e-mail distribution has occurred, and subsequent re-infections of BubbleBoy will not spread again from the same machine. An updated version 1.1 of the program — has now been posted on a Web page hosted in Japan devoted to collecting viruses. A look at the virus reveals a few more details about the program.

Microsoft has a fix for BubbleBoy at: http://www.microsoft.com/msdownload/iebuild/scriptlet/en/scriptlet.htm. Users who have installed Microsoft's patch for the flaw (available from this Web site) are not vulnerable to BubbleBoy, but they may be vulnerable to other HTML/e-mail attacks.

**FunLove:** The virus, technically called W32.FunLove, uses a new strategy to attack the Windows NT file system, in that it attacks the Windows NT file security system and patches the Windows NT kernel.

The virus appears as an executable file running on Windows 95/98/NT. A way to recognize that a machine has been infected is by finding the fclss.exe in the Windows System directory

In order for the virus to completely infect a system, it needs administrative rights on an NT server or workstation. Once an administrator logs on to NT, the virus modifies the NT kernel so that every user has administrative rights to that machine, regardless of the protection.

This means that a "guest" -- someone with the lowest possible rights on the system -- would be able to read and modify all files, including files normally accessible only by the administrator.

**XM/Laroux-KX and XM97/Laroux-KX:** This is a variant of the Excel macro virus and infects Microsoft Excel spreadsheets. In a mixed Microsoft Office environment (for instance, Office 95, Office 97, Office 98, Office 2000) it is possible to have an infection of both XM/Laroux-KX and XM97/Laroux-KX in one spreadsheet.

**WM97/Footer-J:** This Word macros virus attempts to overwrite existing footers or insert a new footer into all open Word documents with the infected document's path and filename.

**W97M/Class.ED:** This is a macro virus (which in reality is made up of two macros) that infects all open Word 97 documents and templates. The polymorphic routine of the virus inserts a line of comment for each line of virus code, in which it includes the following information: date of infection, time of infection, default printer installed, user name, sdjw3456ot76 weor9w5834583, and the system date and time. The virus infects the global template when an infected document is opened. During infection, the virus exports its code to the C:\SYSTEM.SYS file and copies itself to the NORMAL.DOT template. From that moment on, all documents that are closed will be infected by the virus, which imports its code from the C:\ SYS.SYS file and inserts it in the document.

On the 15th of each month, the virus activates its destructive payload, which consists of removing the following options from the "File" menu: "Page Setup...", "Print Preview", Print…", "Exit", New...", Open…", and "Close".

## *Trojans*

The following table provides the reader with a list of Trojans that have received write-ups in this publication. This table starts with Trojans discussed in CyberNotes #99-20 and will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks.

| Trojan | Version | Issue discussed |
|---|---|---|
| Backdoor | 0.1 | CyberNotes 99-21 |
| Bla | 1.0-2.0 | CyberNotes 99-22 |
| BladeRunner | | CyberNotes 99-22 |
| Bobo | | CyberNotes 99-20 |
| BrainSpy | Beta | CyberNotes 99-21 |
| Deepthroat | 3.1 | CyberNotes 99-20 |
| Doly | 1.1-1.6 | CyberNotes 99-20 |
| Donald Dick | 1.53 | CyberNotes 99-22 |
| Donald Dick | 1.52 | CyberNotes 99-20 |
| Eclipse 2000 | | CyberNotes 99-20 |
| **InCommand** | **1.0 (added 1.2)** | **Current Issue** |
| Ini Killer | 2.0-3.0 | CyberNotes 99-21 |
| Irc3 | | CyberNotes 99-21 |
| Logged | | CyberNotes 99-21 |
| Matrix | 1.4-1.5 | CyberNotes 99-20 |
| Millennium | 1.0-2.0 | CyberNotes 99-21 |
| Naebi | 2.12-2.34 | CyberNotes 99-22 |
| NetSphere | 1.0-1.31337 | CyberNotes 99-20 |
| NetSpy | 1.0-2.0 | CyberNotes 99-22 |
| Phaze Zero | 1.0b - 1.1 | CyberNotes 99-23 |
| Revenger | 1.0 | CyberNotes 99-23 |
| RingZero | | CyberNotes 99-22 |
| Ripper | | CyberNotes 99-22 |
| SpiritBeta | 1.2f | CyberNotes 99-22 |
| SubSeven | 1.0-2.0 | CyberNotes 99-21 |
| Thing | 1.00 - 1.60 | CyberNotes 99-23 |
| Transmission Scout | 1.1 - 1.2 | CyberNotes 99-23 |
| Vampire | 1.0 - 1.2 | CyberNotes 99-23 |
| WarTrojan | 1.0-2.0 | CyberNotes 99-21 |
| Xplorer | 1.20 | CyberNotes 99-21 |
| **Xtcp** | **2.0-2.1** | **Current Issue** |
| Y2K Countdown (Polyglot) | | CyberNotes 99-20 |

**InCommand 1.2 (November 1999):** This has the standard file transfer, program control and registry editing ability, but does have potential to be damaging.

**Xtcp 2.1 (November 1999):** This Trojan opens a "shell" on a windows machine. This shell allows an unauthorized user to telnets to your machine and issue various commands.